UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/743,784	12/24/2003	Harold J. Johnson	201371-05000	6160

41018 7590 09/10/2007

CASSAN MACLEAN
307 GILMOUR STREET
OTTAWA, ON K2P 0P7
CANADA

EXAMINER	
LOUIE, OSCAR A	
ART UNIT	**PAPER NUMBER**
2136	

MAIL DATE	DELIVERY MODE
09/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/743,784	JOHNSON ET AL.	
	Examiner	Art Unit	
	Oscar A. Louie	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12-14,16-26 and 30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,12-14,16-21,23-26 and 30* is/are rejected.

7)☒ Claim(s) *22* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This first non-final action is in response to the original filing of 12/24/2003. Claims 1-10, 12-14, 16-26, & 30 are pending and has/have been considered as follows.

Examiner's Note

1. The Applicant appears to be attempting to invoke 35 U.S.C. 112 6th paragraph in Claim 26 by using "means-plus-function" language. However, the Examiner notes that the only "means" for performing these cited functions in the specification appears to be computer program modules. While the claims pass the first test of the three-prong test used to determine invocation of paragraph 6, since no other specific structural limitations are disclosed in the specification, the claims do not meet the other tests of the three-prong test. Therefore, 35 U.S.C. 112 6th paragraph has not been invoked when considering these claims below.

Claim Objections

2. Claims 5, 8, & 26 are objected to because of the following informalities:

- Claims 5, 8, & 26 in line 1 all recite the term "operable" which should be "...configured..." for the purposes of clarification. The examiner notes that the use of the term "operable" is indefinite and may even render limitations as being inoperable. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. The term "high-quality" in claim 6 is a relative term which renders the claim indefinite. The term "high-quality" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-4, 9, 10, 12-14, 17-21, 23-26, & 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shinn (US-6655585-B2) in view of Chow et al. (US-6779114-B1).

Claim 1:

Shinn discloses a method of biometric verification, an electronic device operable for biometric verification, and a computer readable memory medium for storing software code executable comprising,

- "establishing parameters of a software application" (i.e. "When the person attempts to access the system, the application collects new data") [column 1 lines 37-38];
- "generating a biometric template from a set of user's initialization biometric data" (i.e. "A person enrolls by donating some number of samples of the biometric. From these samples, the biometric system creates a model of the particular individual's patterns, which is referred to as a template") [column 1 lines 34-37];
- "generating an access software application based on said software application parameters and said biometric template" (i.e. "When the person attempts to access the system, the application collects new data") [column 1 lines 37-38];

but does not disclose,

- "securing said access software application using tamper-resistant software techniques"
- "thereby allowing said access software application to be stored locally, yet be secure"

however, Chow et al. do disclose,

- "Another aspect of the invention is broadly defined as a method of increasing the obscurity and tamper-resistance of computer software code" [column 9 lines 42-45];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "securing said access software application using tamper-resistant software techniques" and "thereby allowing said access software application to be stored locally, yet be secure," in the invention as disclosed by Shinn for the purposes of "increase the tamper-resistance of the computer software code" [column 6 lines 63-64].

Claim 2:

Shinn and Chow et al. disclose a method of biometric verification, as in Claim 1 above, further comprising,

- "querying a user to input multiple initialization copies of a biometric feature" (i.e. "Typically, biometric systems have a common methodology, regardless of their modality, such as fingerprint, face, voice, or the like. A person enrolls by donating some number of samples of the biometric") [column 1 lines 33-34];
- "reading said multiple initialization copies" (i.e. "From these samples, the biometric system creates a model of the particular individual's patterns, which is referred to as a template") [column 1 lines 34-37];
- "calculating a biometric template based on said multiple initialization copies" (i.e. "From these samples, the biometric system creates a model of the particular individual's patterns, which is referred to as a template") [column 1 lines 34-37].

Claim 3:

Shinn and Chow et al. disclose a method of biometric verification, as in Claim 2 above, further comprising,

- "calculating a biometric template using pattern recognition techniques" (i.e. "From these samples, the biometric system creates a model of the particular individual's patterns, which is referred to as a template") [column 1 lines 34-37].

Claim 4:

Shinn and Chow et al. disclose a method of biometric verification, as in Claim 1 above, further comprising,

- "storing said biometric template in a format different than that required at the input to said access software application" (i.e. "In such authentication systems, cardholder bio-specimens are stored in digital format in the system computer") [column 1 lines 56-58].

Claim 9:

Shinn and Chow et al. discloses a method of biometric verification, as in Claim 1 above, but their combination do not disclose,

- "encoding said access software application using data flow encoding"

however, Chow et al. do disclose,

- " In broad terms, the invention provides for a method of increasing the tamper-resistance of an input piece of computer software code by adding fake-robust data-driven control transfers to that input computer software code" [column 12 lines 10-13];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "encoding said access software application using data flow encoding," in the invention as disclosed by Shinn since "if a large number of control transfers are added to the software code, it will be extremely difficult for the attacker to identify the specific line of control that he wishes to modify" [column 12 lines 24-27].

Claim 10:

Shinn and Chow et al. discloses a method of biometric verification, as in Claim 5 above, but their combination do not disclose,

- "obscuring the data in said biometric template"

however, Chow et al. do disclose,

- "The invention increases the complexity of the control flow by orders of magnitude, obscuring the flow of its algorithm and preventing the attacker from identifying and tampering with targeted areas" [column 6 lines 11-13];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obscuring the data in said biometric template," in the invention as disclosed by Shinn for the purposes of "preventing the attacker from identifying and tampering with targeted areas" [column 6 lines 11-12].

Claim 12:

Shinn and Chow et al. discloses a method of biometric verification, as in Claim 5 above, but their combination do not disclose,

- "encoding the data flow in said access software application into a domain which does not have a corresponding semantic structure, to increase the tamper-resistance and obscurity of said access software application"

however, Chow et al. do disclose,

- "a method of increasing the obscurity and tamper-resistance of computer software code comprising the step of converting its control instructions from its original form, in which the stereotyped control structures provided by human limitations and the limited, fixed

repertoire of high-level control facilities provided in a high-level software language reveal the semantic content and intent of the software code, into a new domain without any such corresponding high-level semantic structure, so that the control structure is divorced both from the original intent of the programmer, and from the forms of control structure easily understood by a programmer reading the code" [column 6 lines 32-42];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "encoding the data flow in said access software application into a domain which does not have a corresponding semantic structure, to increase the tamper-resistance and obscurity of said access software application," in the invention as disclosed by Shinn so that the control structure is divorced both from the original intent of the programmer, and from the forms of control structure easily understood by a programmer reading the code [column 6 lines 39-42].

Claim 13:

Shinn and Chow et al. discloses a method of biometric verification, as in Claim 1 above, but their combination do not disclose,

- "encoding said access software application using control flow encoding"

however, Chow et al. do disclose,

- "Control-flow describes the manner in which execution progresses through the software code. The invention increases the complexity of the control flow by orders of magnitude, obscuring the flow of its algorithm and preventing the attacker from identifying and tampering with targeted areas" [column 6 lines 8-13];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "encoding said access software application using control flow encoding," in the invention as disclosed by Shinn for the purposes of "preventing the attacker from identifying and tampering with targeted areas" [column 6 lines 11-12].

Claim 14:

Shinn and Chow et al. discloses a method of biometric verification, as in Claim 5 above, but their combination do not disclose,

- "obscuring said step of comparing in said access software application"

however, Chow et al. do disclose,

- "The invention increases the complexity of the control flow by orders of magnitude, obscuring the flow of its algorithm and preventing the attacker from identifying and tampering with targeted areas" [column 6 lines 11-13];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "obscuring said step of comparing in said access software application," in the invention as disclosed by Shinn for the purposes of "preventing the attacker from identifying and tampering with targeted areas" [column 6 lines 11-12].

Claim 17:

Shinn and Chow et al. discloses a method of biometric verification, as in Claim 5 above, but their combination do not disclose,

- "adding fake-robust control transfers to said access software application, to increase the tamper-resistance of said access software application"

however, Chow et al. do disclose,

- "adding fake-robust control transfers to the computer software code, to increase the tamper-resistance of the computer software code" [column 6 lines 45-47];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "adding fake-robust control transfers to said access software application, to increase the tamper-resistance of said access software application," in the invention as disclosed by Shinn for the purposes of increasing the tamper-resistance of the computer software code [column 6 lines 46-47].

Claim 18:

Shinn and Chow et al. discloses a method of biometric verification, as in Claim 1 above, but their combination do not disclose,

- "encoding said access software application using mass data encoding"

however, Chow et al. do disclose,

- "If a large number of control transfers are added to the software code, it will be extremely difficult for the attacker to identify the specific line of control that he wishes to modify" [column 12 lines 23-26];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "encoding said access software application using mass data encoding," in the invention as disclosed by Shinn for the purposes of making it extremely difficult for an attacker to identify specific lines of control, thus deterring modification.

Claim 19:

Shinn and Chow et al. discloses a method of biometric verification, as in Claim 5 above, but their combination do not disclose,

- "encoding said biometric template, using mass-data encoding techniques"

however, Chow et al. do disclose,

- "If a large number of control transfers are added to the software code, it will be extremely difficult for the attacker to identify the specific line of control that he wishes to modify" [column 12 lines 23-26];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "encoding said biometric template, using mass-data encoding techniques," in the invention as disclosed by Shinn for the purposes of making it extremely difficult for an attacker to identify specific lines of control, thus deterring modification.

Claim 20:

Shinn and Chow et al. discloses a method of biometric verification, as in Claim 5 above, but their combination do not disclose,

- "responding to a request to store a data value at a virtual address"
- "mapping said virtual address onto a randomly selected actual address"
- "storing said data value in a memory location indexed by said actual address"

however, Chow et al. do disclose,

- "a computer readable memory medium, storing computer software code executable to perform the steps of: re-sorting assignments in said computer software code without changing the semantic operation of said program; copying multiple different overlapping

segments of said computer software code into new segments; and adding fake-robust control transfers to said new segments, to increase the tamper-resistance of said computer software code" [column 6 lines 66-67 & column 7 lines 1-6];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "responding to a request to store a data value at a virtual address" and "mapping said virtual address onto a randomly selected actual address" and "storing said data value in a memory location indexed by said actual address," in the invention as disclosed by Shinn for the purposes of increasing the tamper-resistance of said computer software code [column 7 lines 5-6].

Claim 21:

Shinn discloses a method of biometric verification, as in Claim 1 above, but do not disclose,

- "encoding said access software application using white box encoding"

however, Chow et al. do disclose,

- "In broad terms, the invention provides for a method of increasing the tamper-resistance of an input piece of computer software code by adding fake-robust data-driven control transfers to that input computer software code" [column 12 lines 10-13];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "encoding said access software application using white box encoding," in the invention as disclosed by Shinn for the purposes of increasing tamper-resistance of an input piece of software code.

Claim 23:

Shinn and Chow et al. discloses a method of biometric verification, as in Claim 5 above, but their combination do not disclose,

- "identifying functions and transforms substantive to the targeted software program"
- "generating new functions and transforms which alter the processing activity visible to the attacker"
- "replacing those identified functions and transforms with the new functions and transforms in the software program"

however, Chow et al. do disclose,

- "adding fake-robust control transfers to the computer software code, to increase the tamper-resistance of the computer software code" [column 6 lines 45-47];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "identifying functions and transforms substantive to the targeted software program" and "generating new functions and transforms which alter the processing activity visible to the attacker" and "replacing those identified functions and transforms with the new functions and transforms in the software program," in the invention as disclosed by Shinn for the purposes of increasing the tamper-resistance of the computer software code [column 6 lines 46-47].

Claim 24:

Shinn and Chow et al. discloses a method of biometric verification, as in Claim 1 above, but their combination do not disclose,

- "the level of obscurity is sufficient to make attacks on stored biometric and template prohibitively expensive for attackers"

however, Chow et al. do disclose,

- "Togetherness--Software code or data exhibits togetherness when variables or control flow are so combined that changing individual variables or individual steps in control flow so as to effect a desired change in behaviour, is difficult or infeasible" [column 12 lines 4-8];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the level of obscurity is sufficient to make attacks on stored biometric and template prohibitively expensive for attackers," in the invention as disclosed by Shinn for the purposes of making it difficult or infeasible to make changes in the behavior of the software.

Claim 25:

Shinn and Chow et al. disclose a method of biometric verification, as in Claim 1 above, but their combination do not disclose,

- "said step of securing is performed after said step of establishing parameters of a software application"
- "securing said access software application by applying tamper-resistant software techniques to said parameters"

however, Chow et al. do disclose,

- "Another aspect of the invention is broadly defined as a method of increasing the tamper-resistance of computer software code comprising the steps of: adding fake-robust control transfers to the computer software code, to increase the tamper-resistance of the computer software code" [column 9 lines 42-45];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "said step of securing is performed after said step of establishing parameters of a software application" and "securing said access software application by applying tamper-resistant software techniques to said parameters," in the invention as disclosed by Shinn for the purposes of providing tamper-resistance at the earliest point in time possible.

8. Claims 5-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shinn (US-6655585-B2) in view of Chow et al. (US-6779114-B1) and in further view of a well known feature in the art of cryptography in which official notice is taken.

Claims 5-7:

Shinn and Chow et al. disclose a method of biometric verification, as in Claim 1 & 5 above, further comprising,

- "challenging said user to input an access copy of said biometric feature" (i.e. "") [column 1 lines 38-41];
- "comparing said input access copy of said biometric feature to said biometric template" (i.e. "") [column 1 lines 38-41];
- "responding to said input access copy being a match" (i.e. "") [column 1 lines 45-47];

but Shinn does not disclose,

- "generating a secure password from said biometric template"
- "updating said biometric template"
- "otherwise, generating an incorrect password"
- "generating a high-quality cryptographic key"
- "generating the private key of a public/private key pair"

however, the examiner notes that the applicant appears to be claiming public key/private key pair encryption in Claims 5-7, where a secure password is equivalent with a private key, which is a cryptographic key. Thus, official notice is taken that it is old and well known in the art of cryptography to use public key/private key pair encryption for securing the communication of data/information (as is evidenced by Kaliski, Jr. US-6085320-A in column 1 lines 24-30). Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "generating a secure password from said biometric template" and "updating said biometric template" and "otherwise, generating an incorrect password" and "generating a high-quality cryptographic key" and "generating the private key of a public/private key pair," in the invention as disclosed by Shinn for the purposes of providing secure communications.

9. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shinn (US-6655585-B2) in view of Chow et al. (US-6779114-B1) and in further view of Scott et al. (US-6484260-B1).

Claim 8:

Shinn and Chow et al. disclose a method of biometric verification, as in Claim 5 above, but their combination do not disclose,

- "generate different secure passwords corresponding to different verification thresholds"

however, Chow et al. do disclose,

- "In programmable PID's, verification for individual users can be set at various threshold levels to account for users who may have very fine, worn or damaged fingers. In this event the ease of use can be enhanced by reducing their verification threshold. Verification threshold can be set at the time of enrollment" [column 10 lines 29-34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "generate different secure passwords corresponding to different verification thresholds," in the invention as disclosed by Shinn and Chow et al. for the purposes of providing different access levels and tolerance for users who may have very fine, worn or damaged fingers.

10. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shinn (US-6655585-B2) in view of Chow et al. (US-6779114-B1) and in further view of Chow et al. (US-6594761-B1).

Claim 16:

Claim 8:

Shinn and Chow et al. (US-6779114-B1) disclose a method of biometric verification, as in Claim 5 above, but their combination do not disclose,

- "dispersing subsequences of instructions within said access software application into a plurality of locations"
- "merging multiple dispersed subsequences into single blocks of code"
- "selecting said subsequences of instructions from merged blocks of code for either functionally effective or decoy execution, as needed, to separate the observable operation of resulting code from the intent of the original software during execution"

however, Chow et al. (US-6594761-B1) do disclose,

- "In contrast, the invention disperses the definition of a single variable into several locations so that a single modification or deletion in any one of those locations will corrupt its value" [column 11 lines 33-37];
- "The original program is protected by merging it with this cascade, by intertwining the two. The intention is to make it very difficult for the attacker to separate the original program from the complex wall again, which is necessary to alter the original program" [column 2 lines 36-40];

- "This property is desirable as it magnifies the detrimental effects of any tampering. Of the techniques described herein, Residue Number, Bit-Explosion and Custom Base have this property" [column 11 lines 37-40];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "generate different secure passwords corresponding to different verification thresholds," in the invention as disclosed by Shinn and Chow et al. (US-6779114-B1) for the purposes of making it very difficult for the attacker to separate the original program from the complex wall again due to the magnification of the detrimental effects of any tampering.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
08/27/2007

Nasser Moazzami
Supervisory Patent Examiner

8/27/07